

COLUMBIA POLICE DEPARTMENT

Policy Manual

342 DEPARTMENT TECHNOLOGY USE**342.1 PURPOSE AND SCOPE**

This policy describes the use of department computers, software and systems.

342.1.1 PRIVACY POLICY

Any member utilizing any computer, electronic storage device or media, Internet service, telephone service, information conduit, system or other wireless service provided by or funded by the Department expressly acknowledges and agrees that the use of such service, whether for business or personal use, shall remove any expectation of privacy that the member, as sender or recipient of any communications utilizing such service might otherwise have, with any such communications. The Department also expressly reserves the right to access and audit any and all communications, including content that is sent, received and/or stored through the use of such service.

342.2 DEFINITIONS

Definitions related to this policy include:

Computer system - Includes all computers (on-site and portable), hardware, software and resources owned, leased, rented or licensed by the Columbia Police Department that are provided for use by department members.

Hardware - Includes, but is not limited to, computers, computer terminals, network equipment, modems or any other tangible computer device generally understood to comprise hardware.

Software - Includes, but is not limited to, all computer programs and applications, including shareware. This does not include files created by the individual user.

Temporary file, permanent file or file - Includes any electronic document, information or data residing or located, in whole or in part, on the system, including but not limited to, spreadsheets, calendar entries, appointments, tasks, notes, letters, reports or messages.

342.3 SYSTEM INSPECTION OR REVIEW

There is no expectation of privacy regarding files contained in or on department computers or systems. A department supervisor or the authorized designee has the express authority to inspect or review the system, any and all temporary or permanent files and related electronic systems or devices and any contents thereof, whether such inspection or review is in the ordinary course of his/her supervisory duties or based on cause.

When requested by a member's supervisor, or during the course of regular duties requiring such information, a member of the agency's information systems staff may extract, download or otherwise obtain any and all temporary or permanent files residing or located in or on the system.

Reasons for inspection or review may include, but are not limited to, system malfunctions, problems or general system failure, a lawsuit against the agency involving the member or related to the member's duties, an alleged or suspected violation of any department policy, request for disclosure of data, or a need to perform or provide an agency service.

342.5 UNAUTHORIZED SOFTWARE

To reduce the risk of an agency computer virus, members should not install any unauthorized software onto the computers owned or operated by the Department. If a member must copy data onto a removable storage media and download it on a non-department computer, the member shall scan the removable storage media for viruses before loading the data on a department computer system.

342.6 PROHIBITED AND INAPPROPRIATE USE

An Internet site containing information that is not appropriate or applicable to department use and that shall not be intentionally accessed includes, but is not limited to, adult forums, pornography, chat rooms and similar or related websites. Certain exceptions may be permitted with the approval of a supervisor as a function of an assignment.

342.7 PROTECTION OF DEPARTMENT SYSTEMS AND FILES

All members have a duty to protect the system and related systems and devices from physical and environmental damage and are responsible for the correct use, operation, care and maintenance of the system.

It is expressly prohibited for a member to allow an unauthorized user to access the system at any time or for any reason.